不是会员，如何下载超星主站上的收费书？
在斗争愈加激烈的今天，BE 对超星主站和教育站失效了吗？
本文将给你一个满意的答复！

[注意]

1. 如果你是高手，不必看此文章，因为我说的你都知道。
2. 如果你不屑于本文的观点，说明你是高手，参见第 1 点处理。
3. 如果你对超星毫无了解，也不必看此文章，因为你需要到论坛的置顶贴接受相关知识的教育。
4. 如果你上不了超星教育站，那也请你不必看本文。
5. 本文不会讨论读秀的下载问题，不会讨论关于 SSPARAMS 和 Serverauth 的相关问题，也不会讨论镜像的相关下载问题。（本人没钱买卡，所以无法研究 Serverauth）
6. 我将会用确凿的证据来证明我在此文中的所有观点。

[按]在本文行将写成的时候，在网上读书群里（**********）看到了这样一段对话：

雪上一枝蒿(**********) 23:00:11
进这个群也有数日了，说实在话，能说真话的高手没几个，都在打哈哈。

660(**********) 23:02:08
确实如此，没有什么高手，只有一个所谓的高手就是 007，可惜是一个小人，

雪上一枝蒿(**********) 23:02:33
关于 007 的方法，我今天透露那么一点点，他用的应该是 serverauth, 而不是什么 bookauth
serverauth 是跟用户名相关的
应该说是跟帐号相关的

雪上一枝蒿(**********) 23:07:58
007 用的是动态报头

660 (**********) 23:08:08
只有 007 知道，

雪上一枝蒿(**********) 23:08:48
动态报头的关键是有效帐号

雪上一枝蒿(**********) 23:12:02
顾名思义，动态报头就是在下载每一个文件的时候验证有效的报头(动态的)，与有效帐号相关

660 (**********) 23:12:57
那我问你一下，如果是正版用户就可以下读秀了吗

雪上一枝蒿(**********) 23:14:38
至于说什么有 SS 号还无法得到真实地址的，那都是鬼话。
有 SS 号我可以轻而易举地得到真实地址

雪上一枝蒿(**********) 23:15:40
正版用户理论上应该可以下载 DX，但我没试过
没有真实地址，我可以说任何人都没法下载

雪上一枝蒿(**********) 23:21:45
我只是猜测，动态报头最相关的就是 serverauth

660 (**********) 23:22:53
在正版用户的 serverauth 是固定的

雪上一枝蒿(**********) 23:24:57
动态报头似乎跟 bookauth 无关

007 (**********) 23:28:22
007 报到

雪上一枝蒿(**********) 23:30:02
007 你说实话，你用的是不是动态报头

拽拽(**********) 23:30:29
没有动态报头这个概念

007 (**********) 23:30:49
你说什么动态报头

雪上一枝蒿(**********) 23:30:59
应该说有，我以前实验过

007 (**********) 23:31:17
雪上是高手呀

拽拽(**********) 23:31:20
只有一夫一妻或者一夫多妻的说法　当然是现在

007 (**********) 23:32:11
通过 ssnum 计算一个 bookauth 就可以下载的

雪上一枝蒿(453457691) 23:32:17
一夫一妻制相信大家都知道吧，转基因的结果

007(**********) 23:33:40
serverauth 固定，bookauth 可以通过 ssnum 和用户名计算出来，可以下载读秀任意书

雪上一枝蒿(**********) 23:33:56
有什么问题吗？要政审？

拽拽(**********) 23:34:15
随便问问

无影(**********) 23:34:33

但是计算的难度大了把吧

Danny(**********) 23:34:54

有 bookauth 又如何下？谁教咱一下。

007 (**********) 23:35:07

一个卡用户有一个 serverauth，bookauth 计算出来，下遍读秀任何书

Danny (**********) 23:35:51

用超星算吧

拽拽(**********) 23:35:58

007 就是用这个方法么？

雪上一枝蒿(**********) 23:36:08

我可以说，没有 serverauth，就无法下载 DX

007 (**********) 23:36:31

我是卡用户，有 serverauth

雪上一枝蒿(**********) 23:36:48

除了一夫一妻制

007 (**********) 23:37:34

有超星卡就有 serverauth

007 (**********) 23:38:04

一个超星卡下遍读秀任意书

007(**********) 23:39:20

有 ss 号就可以

雪上一枝蒿(**********) 23:39:53

有卡，等于有有效的 serverauth

拽拽(**********) 23:47:49

007 有工具

无影(**********) 23:47:59

有什么思路

007 (**********) 23:48:07

软件自己写，我是师傅写的软件

无影(**********) 23:49:46

你软件卖不？

007 (**********) 23:49:53

不卖

无影(**********) 23:49:54

换不？

007 (**********) 23:50:06

不换

拽拽(**********) 23:53:07

只要 007 说的 serverauth 固定，bookauth 可以通过 ssnum 和用户名计算出来，可以下载读秀任意书 这思路正确　倒不失又一条下载读秀书的方法

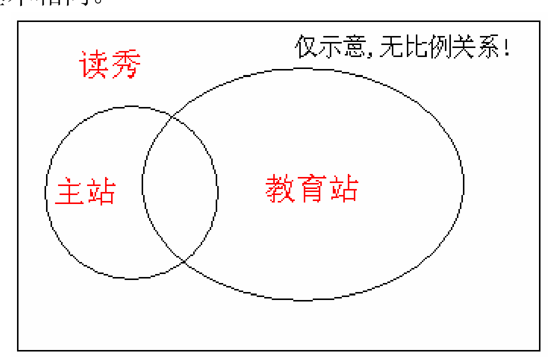
首先明确几个问题：

第一，研究超星的有两类人：第一类人研究的是下载技术，终极目标是毫无限制地把自己想要的所有书籍的最清晰版本下载下来；第二类人研究的是阅读技术，终极目标是毫无限制的阅读所有加密格式的书籍。这两类人不辞辛劳，相互协作，形成了今日超星所面对的百家争鸣、百花齐放的“双百”局面。

第二，由于超星是建立在一个“查漏补缺”的体系之上，所以导致超星从成立之初到现在一直处在与其研究者“魔高一尺，道高一丈”的对峙局面中。旧的漏洞补上了，新的漏洞又产生了。这是我们得以持续下载的基础。感谢超星的漏洞！

第三，超星主站、超星教育站、参考咨询这四个网站的图书关系是：

读秀与 FirstDRS 基本相同。



第五，由于有很多超密四处活动搜集情报，所以本文的方法只限于 2006-9-2 前后有效。

第六，读完本文，你将凭借手中的两把钥匙，开启超星主站和超星教育站的所有大门。

（本文中 ssreader 代替超星主站；sslib 代替超星教育站；duxiu 代替读秀）

友情提示，如果你不关心超星下载可行性的论证问题，请你直接跳至第二章

第一章 超星下载可行性研究

鉴于本人水平有限，所述的方法只能解决主站和教育站的阅读问题（当然你不必拥有主站的会员卡，注册用户足够），本文不讨论下载读秀和参考咨询。

1.1 什么是 http header 验证？

http header 就相当于你访问网站和下载文件的身份证。论坛里的人把这种验证方式称作“一夫一妻”或“一夫多妻”。有了它，你才能顺利地验明正身，得到访问网站和下载文件的资格。

1.2 如何获得 http header？

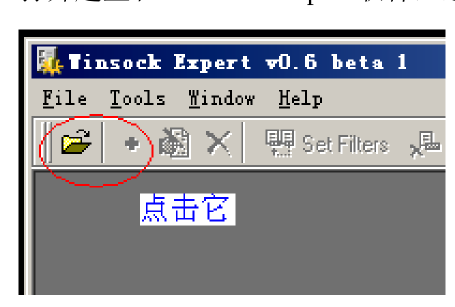
推荐使用 WinSock Expert。

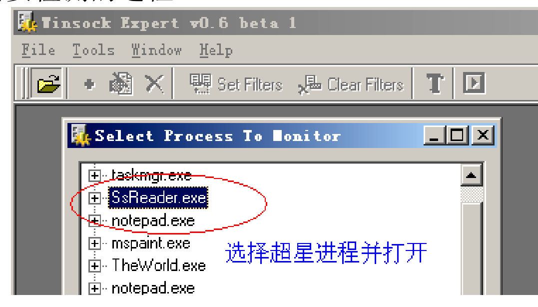
下载地址

http://www.dxqsoft.com/we/index.htm

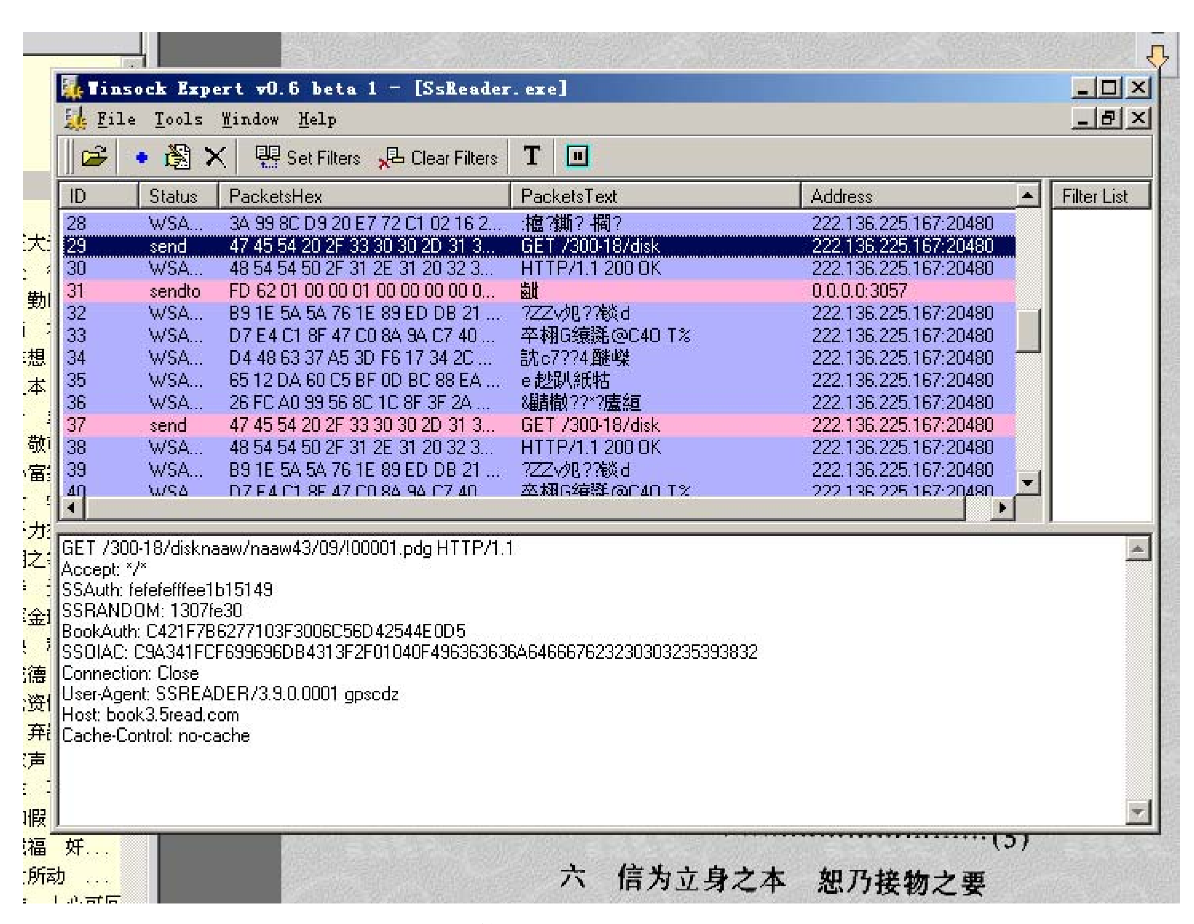
（本软件在使用时会被误认为是病毒，请关掉杀毒软件）

打开超星和 WinSock Expert 软件，选择需要检测的进程 ssreader.exe。





在超星里随便翻一页书，便会得到如下信息：



这里面红色的表示发送的数据包，蓝色的表示接收的数据包。现在我们选择的是第 29 个数据包，里面显示的数据，就是 http header。

GET /300-18/disknaaw/naaw43/09/!00001.pdg HTTP/1.1
Accept: */*
SSAuth: fefefefffee1b15149
SSRANDOM: 1307fe30
BookAuth: C421F7B6277103F3006C56D42544E0D5
SSOIAC: C9A341FCF699696DB4313F2F01040F496363636A64666762323030323539383 2
Connection: Close
User-Agent: SSREADER/3.9.0.0001 readfree
Host: book3.5read.com
Cache-Control: no-cache 可以看出，只要你有了 SSAuth、SSRANDOM、BookAuth、SSOIAC、User-Agent 这五个身份证，你的连接请求 http://book3.5read.com /300-18/disknaaw/naaw43/09/!00001.pdg 就会得到验证，得以成功访问。

如果你是在 IE 里直接敲入这个链接，你的 http header 是不会包含“这么丰富”的身份证的，从而的不到验证，无法成功访问。

1.3 超星的身份证

聪明的你一定想到了，如果能伪造这些身份证，那么，不是就能骗过超星服务器吗？

完全正确，大侠们也不过如此下载的。

超星书籍的所有地址都需要 SSAuth，SSRANDOM，User-Agent 三个字段用来验证。

大部分地址需要 SSAuth，SSRANDOM，User-Agent，SSOIAC 四个字段用来验证。

部分地址需要 SSAuth，SSRANDOM，User-Agent，SSOIAC，BookAuth 五个字段用来验证。

记住，不管怎样，只要你拥有五证，便可以畅通无阻于超星主站和教育站了！

下面我们便来仔细的讲讲超星的每一张身份证。

第一、二张身份证 SSAuth，SSRANDOM

SSAuth: fefefefffee1b15149
SSRANDOM: 1307fe30

这是超星最早期的验证措施，我们不必管它的生成机制及涵义，只需知道：

在超星阅读器里直接访问书籍的真实地址，发出的数据包的 http header 便会自动包含则这两个字段。（真实地址指 http://book3.5read.com /300-18/disknaaw/naaw43/09/!00001.pdg）

BE 可以通过在高级设置里用专用表达式设置。

SSAuth:%AUTH%
SSRANDOM:%RND8_1%

第三张身份证 User-Agent

User-Agent: SSREADER/3.9.0.0001 readfree

大家可以看出，User-Agent 表示的是你的软件名称、版本号和用户名。这个 User-Agent 必须包含完整的版本号和用户名，一定不能错，因为超星在验证第四、五张身份证时，要对这个用户名进行校验的。

第四张身份证 SSOIAC

SSOIAC: C9A341FCF699696DB4313F2F01040F496363636A64666762323030323539383 2

SSOIAC 也就是你在教育站读书时访问每一页书都能看到的链接中的 a，例如

book://read.sslibrary.com/ss2path/ss2path.dll?ssid=11182450&a=C9A341FCF699696DB4313F2F01040F496363636A646667623230303235393832&pagenum=1&pagetype=5

大家看，这个地址的 a 值是不是和 SSOIAC 一样啊！

不仅如此，还透漏给大家一个小秘密：

这个 64 位的 SSOIAC 前 32 位是 C9A341FCF699696DB4313F2F01040F49

后 32 位是 6363636A646667623230303235393832

熟悉读秀的朋友以下便能看出，这后 32 位便是每一本书的 kid！有大侠能够根据这个 kid 推算出这本书的 ss 号呢！而且，每个 ss 号所对应的 kid 不是唯一的！

比如一本名为《维生素女人》的 ssid 是 11271445，而它的 kid 却有好多种！

kid 6A6A6B706A6D6D6E3135323132393339
6565666B656868693135383836373234
63636469636666673830363633393932
61616267616464653138363338383430 ……

SSOIAC 显然与生成它的书籍有关。

SSOIAC 也与时间有关，如果你明天再用今天的 SSOIAC，就会发现它失效啦！

SSOIAC 还和用户名有关，不信你把你 User-Agent 里的用户名改掉，肯定失效的！

但是我要告诉大家一个好消息！超星并不验证 SSOIAC 与书籍的相关性！！！所以在我们的实际使用过程中，SSOIAC 仅与时间和用户名有关！

第五张身份证 BookAuth

BookAuth: C421F7B6277103F3006C56D42544E0D5

这个身份证最重要，也最难获得！俗话说，得中原者得天下；在这里，我也要说，得 BookAuth 者得天下！只要能获得 BookAuth，再配合一个有效的 SSOIAC，不仅超星主站、教育站的书不在话下，甚至连读秀的书也尽收囊中！

限于能力，本人只能得到超星主站和教育站的 BookAuth，但本人将在后面给出证明，为什么从读秀得不到 BookAuth。

经过多次试验证明，BookAuth 与用户名 username 和书籍 ssid 有关。

综上所述，超星的服务器在验证 SSAuth，SSRANDOM 的同时，还要验证 User-Agent，SSOIAC，BookAuth 在用户名 username 上的一致性，以及你所请求的书籍的和 BookAuth 在书籍号 ssid 上的一致性。

只要我们找到一个教育站的 SSOIAC，以及同这个 SSOIAC 的用户名与书籍号相一致 BookAuth，就能把超星主站和教育站的所有图书搬回家！

1.4 为什么无法得到读秀所有书的 BookAuth？

首先应弄明白，超星主站和教育站用的是同一组服务器，唯一的区别是超星主站的图书索引量远远小于教育站。这组服务器的图书地址的共同特征是它们的主机名都形如 book*.*read.com

而读秀和参考咨询用的是另一组服务器，这组服务器的图书地址的共同特征是它们的主机都形如 hn*.*read.com。

这两组服务器所采用的验证机制不同。

超星主站和教育站所采用的是如上述的“五证式”验证机制

（这里不包括有卡用户）

```
GET /300-18/disknaaw/naaw43/09/!00001.pdg HTTP/1.1
Accept: */*
SSAuth: fefefefffee1b15149
SSRANDOM: 1307fe30
BookAuth: C421F7B6277103F3006C56D42544E0D5
SSOIAC: C9A341FCF699696DB4313F2F01040F496363636A646667623230303235393832
Connection: Close
User-Agent: SSREADER/3.9.0.0001 readfree
Host: book3.5read.com
Cache-Control: no-cache
```

而读秀和参考咨询所采用的是下面“四证式”验证机制。

GET /300-06/diskshenzhen/20030315_2/a1001956/000003.pdg HTTP/1.1
Accept: */*
SSAuth: 373737363728789880
SSRANDOM: 03feda5e
SSPARAMS: <?xml version="1.0" encoding="GB2312"?> <SSParam expiredate="2006-8-30"><serverinfo><localaddr>210.41.104.168</localaddr><authcode></authcode><domain></domain></serverinfo><userinfo><name></name><id>0</id><account>0</account></userinfo><bookinfoaddress="687474703A2F2F686E312E35726561642E636F6D2F3330302D30362F6469736B7368656E7A68656E2F32303033303331355F322F61313030313935362F3030303030312E706467"><metadata><ssid>10865918</ssid><title>B8DFB5C8CAFDD1A7D1A7CFB0D6B8B5BC2020B6FE</title></metadata><right><read canread="1" readreg="0" readrange="1-17,1"/><download candownload="0" downloadreg="0" downloadencrypt="0" downloadrange="1-17,1"/><print canprint="0" printreg="0" printrange="1-17,1"/></right></bookinfo><verifyinfo encryptmethod="2" value="BB48E7B8C5A21AB1B28366AB16883F408FB1D4BD"/></SSParam>
User-Agent: SSREAD_WEB/1.0.0001
Host: hn1.5read.com
Connection: Keep-Alive
Cache-Control: no-cache

正是由于以上认证方式的区别，导致了无法得到所有书的 BookAuth。

但是，通过对超星教育站和读秀上都有的书的比较，我发现，只用超星教育站的“五证”，同样可以下载读秀地址的书。我把例子的书名和地址贴在下面，有兴趣的可以试一下：

《易错的英语习惯表达法及详解》
http://www.duxiu.com/book/000/000/626/914/8CCEEA919A76C554894FD0BCA170CF72.htm
ssid=11094167
http://hn2.5read.com/300-26/disklaa/laa73/03/000063.pdg
http://book5.5read.com/300-56/disklaa/laa73/03/000063.pdg

以下是对“无法得到读秀所有书的 BookAuth”的专业解释：

有证据表明 bookauth 是在服务器上生成并下载至本地的。

现在只有 sslib/ssreader 服务器能够生成 bookauth。对于 sslib/ssreader 服务器上没有收录并索引的书，是得不到 bookauth 的。也就是说，即使你能伪造 username，但是要想欺骗 sslib/ssreader 服务器得到任意 ssid 对应的 bookauth，我认为是根本做不到的，因为它的索引数据库里根本没有你要的 ss 号。

所以那些自称能下 duxiu 所有书的人，肯定不是通过 bookauth 这条途径来下书的，他们的方法或者是通过镜像，或者是通过 SSPARAMS、Serverauth……（本文不涉及）

大家在截获报文的时候注意观察以下现象：

点击“阅读器阅读”后，会产生连续的几个发包，其中有一个发包是：

<Request><SSID>11271445</SSID><UserInfo Account="1" name="readfree" HddKey="525316023"/><Operation>Open</Operation><ResVer>0</ResVer><ServerKey><rverKey><AppVer>SSReader/3.9.0.0001</AppVer><UrlAuth>FDBC99EDDF5433C3347EF740319ED0C86565666B6568686931353838363732 34</UrlAuth></Request>

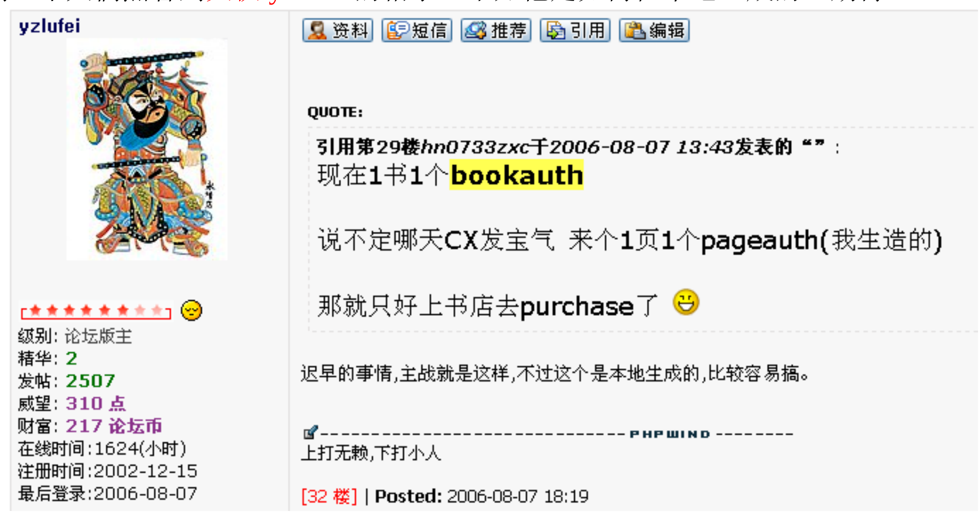
接着会收到两个包。其中一个是很长的乱码，这个乱码里包含有很多关于书的加密信息。此时用内存查看工具查看内存，会发现超星把这段乱码解成了明文并放在内存里:

<Response><Guide><Reference Type="preface" Title="前言页" href="fow001.pdg" pages="-1"/><Reference Type="toc" Title="目录页" href="!00001.pdg" pages="-1"/><Reference Type="text" Title="正文页" href="000001.pdg" pages="105"/><Reference Type="att" Title="附录页" href="att001.pdg" pages="-1"/><Reference Type="bac" Title="封底页" href="bac001.pdg" pages="-1"/></Guide><Right><Read CanRead="1" ReadReg="0"/><Download CanDownload="1" DownloadEncrypt="1" DownloadMode="2" DownloadReg="0"/><Print CanPrint="1" PrintReg="0"/></Right><Metadata><Title>维生素女人</Title><SSID>11271445</SSID><Creator>中国烹

饪协会美食营养专业委员会编著</Creator><Pages>105</Pages><Date>2004 年 07 月第 1 版</Date><Publisher>北京出版社</Publisher></Metadata><Address><Url herf="http://book2.5read.com/300-3/disknrad/nrad02/04/!00001.pdg" Ver="1"/></Address><MediaType>book/graphpdg</MediaType><FullTextSearch/><FileInfo><Auth>FC0A27042C9D82149A706301888F9CC6</Auth></FileInfo></Response>

通过对比可以发现，这个 Response 显然是对发包的 Request 的回应。而注意看<Response>的末尾又能惊奇的发现，原来这里的<Auth>FC0A27042C9D82149A706301888F9CC6</Auth>就是我们日思夜想的 bookauth！所以，我要说我有充足的证据证明 bookauth 是在服务器上生成并下载至本地的。我觉得大家寻找 bookauth 的努力应该到此为止了。

无独有偶，今天偶然看到大侠 yzlufei 的帖子，不知他是如何在本地生成的，期待！



大家也可以去看看！

http://cache.baidu.com/c?word=bookauth&url=http%3A//www%2Ereadfree%2Enet/bbs/read%2Dhtm%2Dtid%2D209083%2Dpage%2De%2Dfpage%2D1%2Ehtml&b=0&a=123&user=baiduadv

http://cache.baidu.com/c?word=bookauth&url=http%3A//www%2Ereadfree%2Enet/bbs/read%2Dhtm%2Dtid%2D209083%2Dpage%2D1%2Dfpage%2D1%2Ehtml&b=0&a=103&user=baiduadv

1.5 其它一些结论

1. ssreader 和 sslib 会给出 SSOIAC，bookauth 以及形如 book*.*read.com 的地址；
   而 duxiu 和 dsr 给出的则是 SSPARAMS 以及形如 hn*.*read.com 的地址
2. 仅仅只凭借 a 值(满足时效性和用户名即可)和 bookauth(必须满足用户名和书)就完全可以搞定形如 book*.*read.com 以及形如 hn*.*read.com 的地址。也就是说，hn*.*read.com 的服务器除了具备验证 SSPARAMS 的功能外，还可以验证 SSOIAC+bookauth。
3. 同一用户（地区）对不同时间的 SSOIAC 是不同的，不可替代的。
   同一本书对不同用户（地区）的 BookAuth 是不同的，不可替代的。
   并且 SSOIAC，BookAuth 是与 User-Agent 的版本号与用户名有关。
4. 任何一种能自定义 HTTP Header（中文应叫做“HTTP 报头”）的下载工具均可下载 cx 图书。目前常见的此类工具有 BE，wget 等等，

第二章　超星下载的准备工作

根据第一章的理论准备，我们得到如下有用结论：

1. duxiu 和 dsr 是全集，ssreader 和 sslib 的并集是他们的一个子集。由于缺少 bookauth，他们的差集无法搞定。
2. 只需五证齐全，便可以搞定 ssreader 和 sslib 的并集。即只要我们找到一个教育站的 SSOIAC，以及同这个 SSOIAC 的用户名与书籍号相一致 BookAuth，就能把超星主站和教育站的所有图书搬回家！

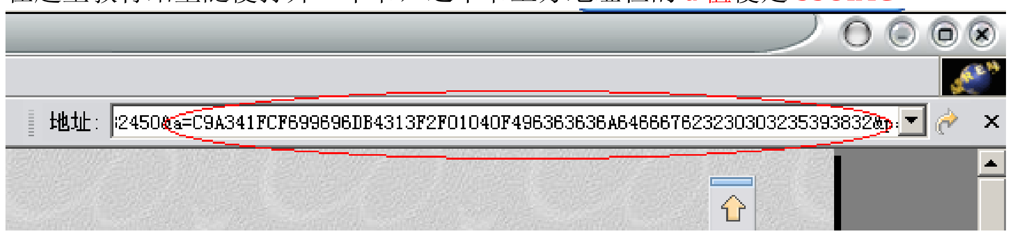
2.1 如何获取这几张身份证

第一、二、三张身份证 SSAuth，SSRANDOM，User-Agent

不需获取，软件自动生成。需记住用户名。

第四张身份证 SSOIAC

在超星教育站里随便打开一本书，这本书上方地址栏的 a 值便是 SSOIAC



book://read.sslibrary.com/ss2path/ss2path.dll?ssid=11182450&a=C9A341FCF699696DB4313F2F01040F496363636A646667623230303235393832&pagenum=1&pagetype=5

a=C9A341FCF699696DB4313F2F01040F496363636A646667623230303235393832

这就是我们需要的 SSOIAC。

第五张身份证 BookAuth

这张身份证最难获取，尤其是对于超星主站的新书。当然，只要证明了它能够获取，我们就有办法。

在研究过程中我发现，只要超星阅读器的菜单[注册]-[用户信息]里写的是未注册，在主站便无法得到 bookauth。所以我们既需要把用户名换成 SSOIAC 对应的 username，也需要把状态改为其它形式。



这里教大家一个简单的办法，比如我们要下的书的 ssid 是：11271445

第一步：把下面的文字贴进记事本里

```
	<Script language="JavaScript">
	function CovertCRLFToBR(s)
		{
		 var i;
		 var s2 = s;
		 while(s2.indexOf(".")>0)
		 {
		 i = s2.indexOf(".");
		 s2 = s2.substring(0, i) + s2.substring(i + 1, s2.length);
		 }
		 return s2;
		}
		function isSSPlugInstalled()
		{
			var obj;
			try{
				obj = new ActiveXObject("SSREADERPLUG.SSReaderPlugCtrl.1");
			}catch(e){}
			if(obj != null)
				return true;
			else
				return false;
		}
	</Script>

				<OBJECT id=SSReaderPlug1 style="LEFT: 0px; WIDTH: 0px; TOP: 0px; HEIGHT: 0px"
classid=clsid:3359C0B1-2363-40B3-AFCA-1ABC799AC486
					codebase="http://reg.ssreader.com/SSReaderPlug.cab#version=2,0,0,4"	height=0
width=0>
				  <PARAM NAME="NewVer" VALUE="3.72">
				  <PARAM NAME="NewData" VALUE="2003-05-01">
				  <PARAM NAME="DownloadPath" VALUE="http://www.ssreader.com/download/">
				</OBJECT>

				<SCRIPT LANGUAGE="JavaScript">
					var Param;
					var Ver;
					Ver = SSReaderPlug1.SSReaderVer;
					Ver = Ver.substring(0,10);
					Ver = CovertCRLFToBR(Ver);
					if(Ver>0 && (Ver-3730001) < 0)
					{
							if((Ver-3720001) < 0)	//3.7.2.0001 以前的版本使用 book://ssusereg 的方
法进行注册
							{
								url							=
"book://ssusereg/?isreg=1&username=readfree&regcode=22713c2a5357e3128bbc907d6d06976a94bc1b14627
ade2bf53d75eaaa39e6e3c21d1b6910caed28e9bbef07&errno=20";
								this.location.href = url;
							}
							else				//3.7.2.0001 以后的版本使用控件方法进行注册
```

```
                                    {
SSReaderPlug1.UserRegister("readfree","22713c2a5357e3128bbc907d6d06976a94bc1b14627ade2bf53d75eaaa39e6e3c21d1b6910caed28e9bbef07");
                                    }
                        }
                        else
                        {
SSReaderPlug1.SetRegCode("readfree","22713c2a5357e3128bbc907d6d06976a94bc1b14627ade2bf53d75eaaa39e6e3c21d1b6910caed28e9bbef07","1","2006-06-04");
                        }
                </Script>
    <script>
        window.open('http://reg.ssreader.com/srvcenter.asp','_parent');
    </script>
```

然后将这段文字保存为一个网页文件，如 readfree.htm

这个文字的作用是将“用户信息”修改为你需要的用户名。

第二步，在超星主站随便注册一个用户名，并在超星阅读器中打开超星主站并用此用户名登录。

这一步的作用是得到合法的 cookie 信息。

第三步，将上面保存的这段网页中的 readfree 换成你刚才得到的 SSOIAC 所对应的用户名，

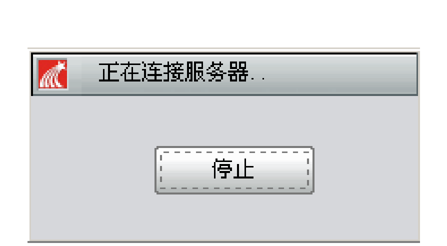
比如是：freeread（一共有三处，换最后两处即可）。

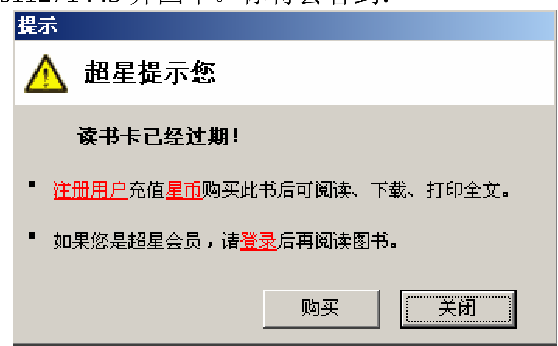
第四步，在超星阅读器里打开这个网页，这时，你会发现右下角升起一个小方框！用户信息也变成了你需要的 freeread。





第五步，在超星浏览器中输入 book://ss11271445 并回车。你将会看到：



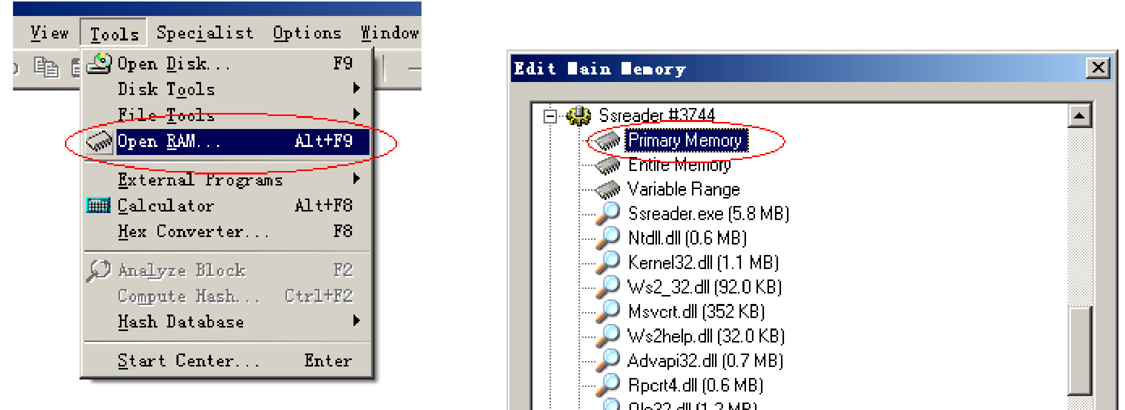


此时，见到超星的提示，你便可以长舒一口气：bookauth 终于被放在内存中了。

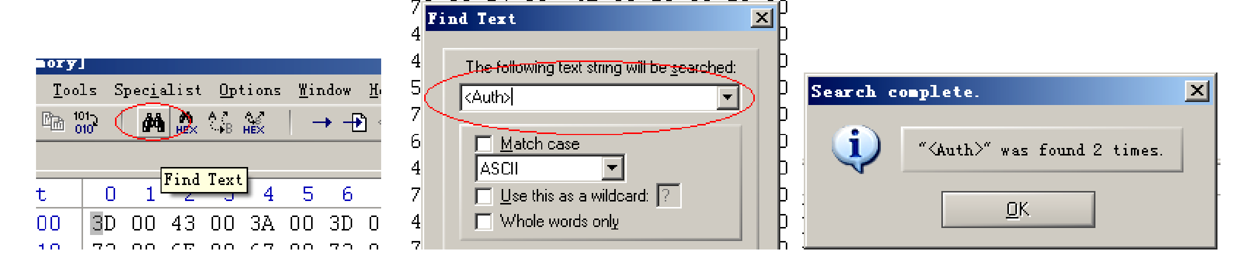
（当然，如果提示 ss 号不在数据库中，那就不在本文讨论范围了）

这时不要试图再去截获什么数据包，因为这些数据是加密传输的。那么怎么找到 bookauth 呢？聪明的你一定想到了，用内存查看工具！我们选择 winhex，非常简单，实用。

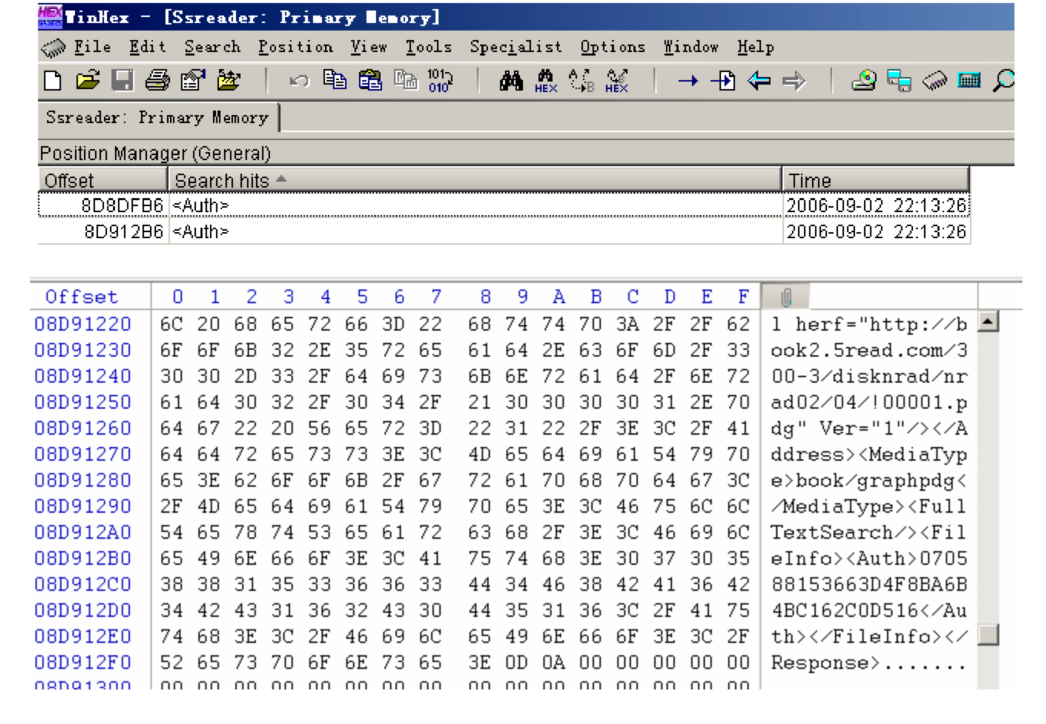
第六步：打开 winhex，在菜单栏里选择[工具][打开内存]，选择“ssreader”进程并选择其中的“主要内存”，确定打开。



第七步，点击“望远镜”工具[查找文本]并键入检索内容<Auth>，并确定。(注意是半角)

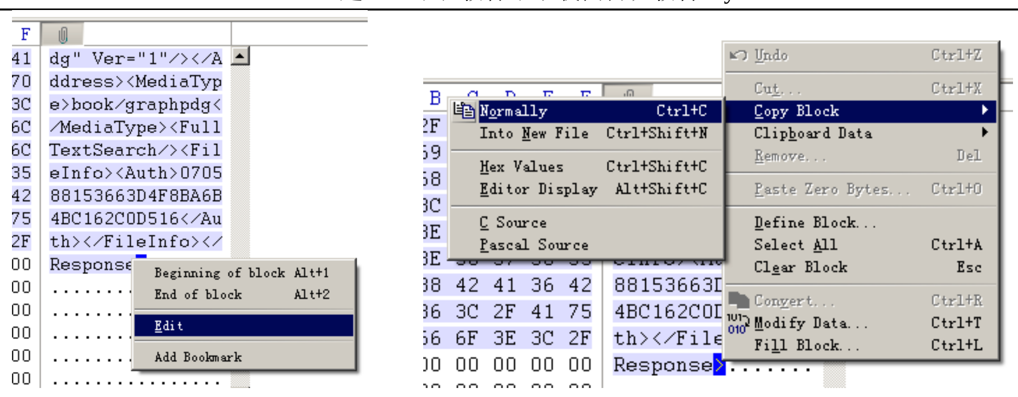


第八步，可以看到，上一步检索出两个结果。选择一个结果就能在内存中看到你要的所有信息，包括下载地址！复制下来！



这一段文字里面会有乱码，别怕，那是中文！

这里的复制过程和其它软件不同，选择复制范围后点击右键，选择[Edit]



然后依次选择[copy Block]---[normally]　(或者选中范围后直接 ctrl+c)，贴于下面：

<Response><Guide><Reference Type="preface" Title=" 前 言 页 " href="fow001.pdg" pages="-1"/><Reference Type="toc" Title="目录页" href="!00001.pdg" pages="-1"/><Reference Type="text" Title="正文页" href="000001.pdg" pages="105"/><Reference Type="att" Title="附录页" href="att001.pdg" pages="-1"/><Reference Type="bac" Title=" 封 底 页 " href="bac001.pdg" pages="-1"/></Guide><Payment><Price>6</Price><Payed>0</Payed><PayAddress>http://reg.ssreader.com/payment/payment.asp</PayAddress></Payment><Right><Read CanRead="1" ReadReg="1"/><Download CanDownload="1" DownloadEncrypt="2" DownloadReg="1"/><Print CanPrint="1" PrintReg="1"/></Right><Metadata><Title>维生素女人</Title><SSID>11271445</SSID><Creator>中国烹饪协会美食营养专业委员会编著</Creator><Pages>105</Pages><Date>2004 年 07 月第 1 版</Date><Publisher> 北 京 出 版 社 </Publisher></Metadata><Address><Url herf="http://book2.5read.com/300-3/disknrad/nrad02/04/!00001.pdg" Ver="1"/></Address><MediaType>book/graphpdg</MediaType><FullTextSearch/><FileInfo><Auth>070588153663D4F8BA6B4BC162C0D516</Auth></FileInfo></Response>

如此，我们便得到了很多有用信息！尤其是！

下载地址　http://book2.5read.com/300-3/disknrad/nrad02/04/!00001.pdg

bookauth　<Auth>070588153663D4F8BA6B4BC162C0D516</Auth>

以上是用来对付超星主站的！

对于教育站，可以采用在打开书之后截获数据包的方法，也可采用这种方法。

注意，在使用 winhex 时，如果搜索过程中出错一般是因为内存在变化，重新打开内存搜索即可！

综上所述，我们便得到了这五个重要的身份证以及书的真实地址！

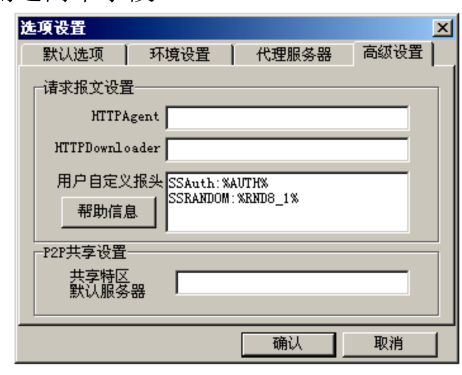
2.2　如何伪装这几张身份证

第一、二张身份证 SSAuth，SSRANDOM

如果你用超星的浏览器看书或下书，不必设置这两个字段。因为在超星阅读器里直接访问书籍的真实地址时，发出数据包的 http header 便会自动包含则这两个字段。

BE 可以通过在高级设置里用专用表达式设置。

```
SSAuth:%AUTH%
SSRANDOM:%RND8_1%
```



第三、四、五张身份证 User-Agent、BookAuth、SSOIAC

User-Agent: SSREADER/3.9.0.0001 readfree
BookAuth: C421F7B6277103F3006C56D42544E0D5
SSOIAC: C9A341FCF699696DB4313F2F01040F496363636A646667623230303235393832
这几张身份证要用软件 Proxomitron 设置。

Proxomitron 又名通用网页过滤器。它相当于一个警卫站在门口（网卡）给每一个出去的人（数据包）发其所需要的身份证（User-Agent、BookAuth、SSOIAC）。

打开 Proxomitron 软件，只选中“发送头部过滤器”。点击[头部]，将所有选项的钩都去掉（因为不需要）。

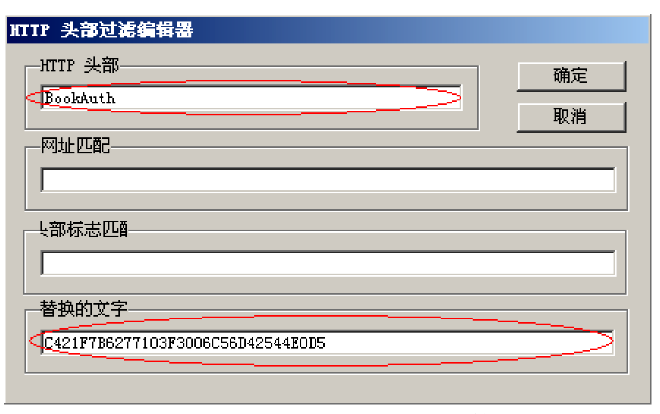


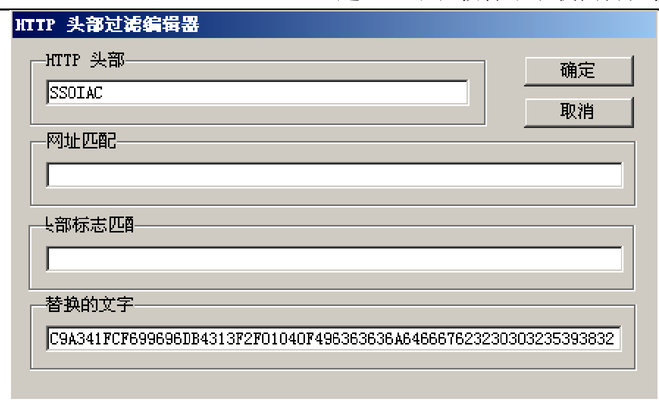


点击[新建]，将 User-Agent 和 SSREADER/3.9.0.0001 readfree 填入并确定。
记得字符串前后要去掉空格。

HTTP 头部过滤编辑器
HTTP 头部
User-Agent
确定
取消
网址匹配
头部标志匹配
替换的文字
SSREADER/3.9.0.0001 readfree

其余两个身份证照此填入





之后选中这三项前面的两个小方框



点击[确定]，回到主界面后先[保存默认设置]，再[中止]一下重新运行。



至此为止，准备工作就做好啦!!!

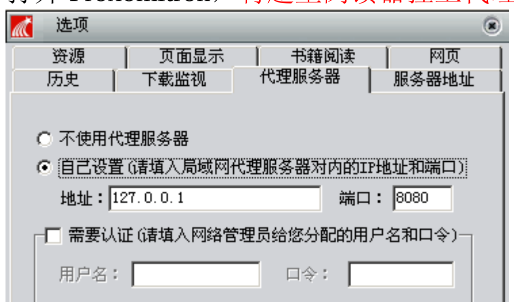
只需要将应用软件的代理设置填为 127.0.0.1:8080，这样从应用软件出去的所有 http header 都会包含这三个身份证的!

第三章　超星下载的两种方法

3.1 下载前的检查

检查设置是否有效的简便方法：

打开 Proxomitron，将超星阅读器挂上代理。

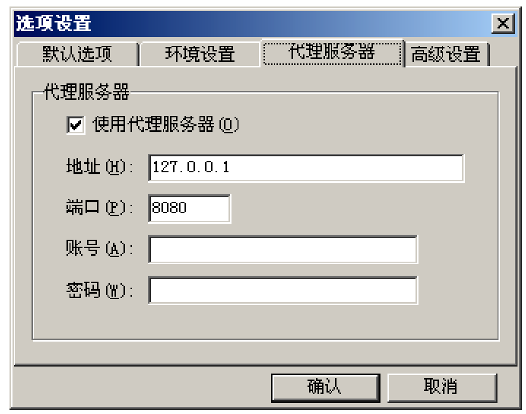


在阅读器的地址栏里输入 http://book2.5read.com/300-3/disknrad/nrad02/04/!00001.pdg 地址并回车。看书，翻页。检查是否成功。

原理： 在超星阅读器中输入类似 http://book5.5read.com/300-56/diskgdr/gdr19/08/!00002.pdg 的地址并回车，此时超星发送的报头中已经包含了 SSAuth，SSRANDOM 这两个字段。然后，这个报头通过 Proxomitron 之后被添加上了 User-Agent，SSOIAC，BookAuth 字段．这样一来发送给超星服务器的报头是完整的。所以这是一种行之有效的检查方法。

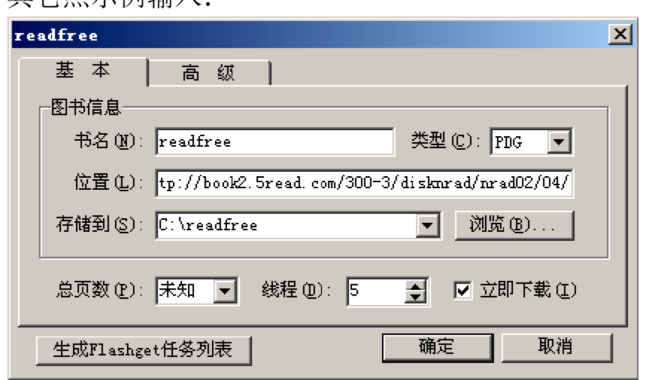
3.2 用 BE 下载

在第二章中，已经对 BE 进行了设置，这里还需要给 BE 挂上代理：



给 BE 添加任务，地址填入 http://book2.5read.com/300-3/disknrad/nrad02/04/

其它照示例输入：



点击[确定]便可以下载了（因为未输入页数，所以便不会有进度显示）。
点中这个任务，会看到上方进度栏和下方进度栏分别用图形和文字显示进度。
过一会便回弹出下载完毕的对话框。
用 BE 下载的缺陷：

1. 会生成*.qdg 文件，将其删除即可！
2. 某些书（尤其是图像 pdg）下载后将会无法打开。一般格式的则没有问题。
   （这是由于 BE 在下载时会修改文件）

3.3 用超星下载

俗话说，原版的才是最正宗的。
在下载上也的确如此。既然能用这种方法在超星阅读器里看书，那么肯定也能下书！
挂上代理，点击右键下载吧！
用超星阅读器下载的缺陷：

1. 需要输入页数，否则它会重复连接至 1000 页。(这很好办)
2. 直接下载至本地的文件将会被保存为 66H 格式的。这时就需要用截留法了。这里推荐一种截留法，是本人认为最有效、最方便的——Web-Sniffer 的汉化增强版。
   在论坛上的下载地址是：
   http://www.readfree.net/bbs/read-htm-tid-198346-keyword-websniffer.html
   相信大家会爱上她的。

2006-9-2

--[The End]--------------------------------

[P.S.] 本人也是从菜鸟走过来的，非常看不惯某些人对待新手的态度，所以写成此文，以让更多新手能尽快入门，让更多没钱读书的人能读上书，读好书！并希望百花齐放、百家争鸣之风在园地盛行！

想想最初的三位大侠 Shun Cox、刘健英、Freereading，他们的精神应该能让如今的某些人汗颜！

尤其是大侠 Shun Cox，他的 Book Exepress 就像越王勾践剑一样历经磨难却仍锋利无比！

有志者事竟成,破釜沉舟,百二秦关终属楚
苦心人天不负,卧薪尝胆,三千越甲可吞吴

一些有用的空间
http://free.ys168.com/?pdg
http://free5.ys168.com/?ssreader
http://free.ys168.com/?tearock